REMARKS

The Applicant thanks the Examiner for his review of the present application and for his comments thereon. Amendments have been effected to the drawings and the specification with respect to rejections raised by the Examiner and to correct typographical errors. The claims have also been amended to clarify the nature of the invention. However, these amendments have not added new subject matter to the application.

Page 2, line 21 to Page 3, line 7 of the summary of the invention has been amended according to the amendments effected to the claims and does not add any new subject matter.

Page 3, line 20 has been amended to maintain consistency with earlier teachings in the specification. Member "B_n" has been replaced with "B_m" as similarly described in the specification on Page 2, line 5. The number of parties in each entity need not be equal, therefore may be defined as m and n where m is not necessarily equal to n.

Page 4, line 21 has been amended in response to the Examiner's objection. Applicant has respectfully replaced "entity" with "member" to address this concern.

The enclosed replacement formal drawing page containing Figure 1 includes the numeral 10 with an arrow directed towards the entirety of the communication system as the numeral 10 has been referred to in the specification, thereby complying with 37 CFR 1.84(p)(5). The enclosed replacement sheet containing Figure 2 has been submitted as a formal drawing.

Claim 1 has been rejected under 35 U.S.C. 112 first paragraph as failing to comply with the enablement requirement. Applicant respectfully submits that claim 1 as amended is fully supported by the specification thereby enabling one skilled in the art to make and/or use the invention.

In the specification, the method claimed according to the present invention has been

exemplified as the case where m = n = 2. The following describes the creation of the shared key K with exemplary support from the specification.

As indicated in the preamble, each member in each entity has respective long-term public and private key pairs as exemplified on Page 3, lines 30-31 of the specification. The operation performed in clause (a) as amended, combines for each entity, the long-term public keys of the members to create an entity long term public key.

The operation performed in clause (b) generates short term private and public key pairs for each member as exemplified on Page 4, lines 13-17 of the description. Clause (c) follows and has been amended to clarify that the short term public keys of clause (b) are made available to the other members of its respective entity which essentially constitutes an exchange of the key but may be done directly or indirectly by way of merely making the keys available to the other members. A supporting example is described on Page 4, lines 18-20.

The short-term public keys are available to the members in their respective entity, as stated in clause (d) sub-step i, and as such, each member computes an intra-entity shared key by combining the short-term public keys of each member as described on Page 4, line 21. Each member also computes, in clause (d) sub-step ii, an intra-entity public key by combining its short term private key, the long-term private key of its respective entity and the intra-entity shared key. This mathematical combination is made by example on Page 4, lines 26-30.

Following the above, clause (e) of claim 1 combines the intra-entity public keys of the members to create a group short-term public key for each entity as exemplified on Page 5, lines 1-3. The method continues with clause (f) which has been amended to clarify that the intra-entity shared key and its long-term public key (i.e. as opposed to its group short term public key) are made available to the other entities.

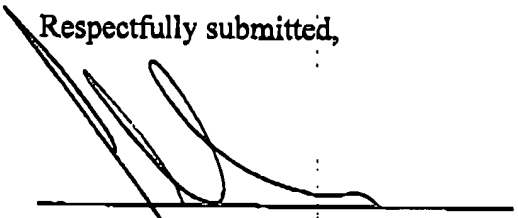
The amendments to clause (f) provide consistency with the mathematical combination made in clause (g) in which each entity computes a common shared key K using the keys made

available by the other entities as stated in clause (f) and using its own group short-term public key computed in clause (e). This computation is clearly described by example on Page 5, lines 9-12.

Accordingly, it is believed that claim 1 as amended contains subject matter which is fully supported by the specification in light of the above exemplary references to the specification and as such is in condition for allowance. Claims 2-11 are either directly or indirectly dependent upon claim 1 and are therefore also believed to be in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: September 27, 2004

Blake, Cassels & Graydon LLP
P.O. Box 25
Commerce Court West
Toronto, Ontario M5L 1A9, Canada

Tel: (416) 863-2400

JRO/BSL/jsm